Modus Operandi

Automating Command Post and Battle Staff Operations at the USAF 45th Space Wing

Robert D. Price
Director Product Services
Modus Operandi, Inc.
bprice@modusoperandi.com

Timothy W. Beltz
Federal Business Unit Manager
ESi Acquisition, Inc.
tbeltz@ESI911.com

2d Lt. Nathan McKinnon
45th Space Wing Communications Squadron
Nathan.McKinnon@patrick.af.mil

Abstract

The DOD Net-Centric strategy seeks to insure that all data are visible, available, and useable when needed and where needed. Data visibility and usefulness are dependent on the development of systems and applications that are network enabled and have the capability to present information in a coherent manner. The current largely paper-driven procedures for installation command post and crisis management activities must give way to more automated processes that allow data to be automatically ingested from many sources available on the network. Moreover, data at the local level needs to be available on the network to other information consumers. Recently, the USAF 45th Space Wing at Patrick Air Force Base installed a low-cost solution for automating Command Post and Battle Staff operations. The system, named Shark Command and Control System (SCCS), is based on WebEOC®, a commercial product created and marketed for emergency operations centers by ESi, Inc. WebEOC was easily adapted to the role of daily command post operations and was already suitable for emergency/crisis management operations. The capabilities provided by WebEOC are significantly enhanced by the Knowledge Management Framework (KMF), which is based on BEA's AquaLogic™ Data Services Platform and Modus Operandi's Wave® product. The KMF allows SCCS to display federated data from a wide variety of data sources, including relational databases and XML documents. The KMF provides a semantic layer on top of the federated data to allow queries to return information based on a domain model that includes classes and relationships between classes. This has allowed SCCS to display data from sources that were formerly "silos" of information. In turn, data accumulated in SCCS is made available to other information consumers via the KMF. This paper describes SCCS and KMF capabilities and looks forward to how command posts can be interconnected and access federated data.

Introduction

Given the DOD commitment to Net-Centric warfare, the creation of unit level command posts that are capable of accessing data and services in a Net-Centric environment is imperative. Command posts also require the capability to be data and service providers to authorized external users. The majority of military units are operating at a permanent installation that is their home base. Temporary deployments are generally the exception to a normal operating environment. There is a need to optimize command post operations in the normal garrison environment and to provide Net-Centric access at all levels of the command structure. Forward deployed command posts such as the Command Post of the Future (CPOF)[1]

[1] Defense Update International Online Defense Magazine. (2005). *Command Post of the Future CPOF*. Retrieved May 26, 2006 from: http://www.defense-update.com/products/c/cpof.htm

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 OCT 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Automating Command Post and Battle Staff Operations at the USAF 45th Space Wing	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Modus Operandi, Inc.**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**7**	

may have different requirements from those of an installation command post.

Basic Command Post Requirements

Most military command post systems must provide a basic set of capabilities that are common to all command post operations. These capabilities include:

- Checklists distilled from Operations Plans
- Event Logs to record significant events
- Display of geo-spatial data
- Authentication via login
- Capability to define users, roles, and groups
- Simulation and training
- Capability to access data from disparate data sources
- Capability to access Net-Centric data services
- Capability to register services for use by others
- Robust security policy governing access to services

In addition, a command post system should have the following characteristics:

- Easy to learn and use
- Easy to administer and maintain
- High reliability
- High performance
- Mobility
- Easy to add new functionality

Net-Centric Requirements

The capability to access data and services from external data and services providers is a key concept of Net-Centric initiative. The goal is to minimize the amount of private data and to increase the amount of community and enterprise data to make data visible, accessible, and understandable.[2] Command posts must do more than simply store event logs and provide data entry. They need to be the commander's window into the data/services cloud made available through the Global Information Grid (GIG) and the Net-Centric framework. Tying the command post into the data/services cloud is essential to avoiding the construction of just another data silo.

A Command Post Implementation - WebEOC

The 45th Space Wing recently brought its Shark Command and Control System (SCCS) into operation. SCCS is a system developed by Modus Operandi, Inc. (MO) under a Small Business Innovation and Research (SBIR) grant from the Air Force Research Laboratory (AFRL). SCCS uses WebEOC to provide the core functionality. WebEOC is produced by Emergency Services Integrators, Inc. (ESi) as a command and control system for emergency operations centers. MO found that WebEOC was easily adapted to a military command post role.

WebEOC is a web-based Crises Information Management System that utilizes a Microsoft SQL database for the real time collection, management and dissemination of information critical to incident response. It was designed to aid decision making and down-channel reporting by providing authorized users real-time information in a user-configurable format. WebEOC is versatile in that it is easily adapted to any command and control role. It not only provides the capability to disseminate emergency information real-time, it is:

- Easy to learn, use and remember. User training can normally be conducted in 15 minutes or less.
- Adaptable to local operations. WebEOC can be adapted to local conduct of operations and does not force users to implement a new way of doing business.
- Offers low implementation and maintenance costs. It does not rely on third party products whose licenses must be renewed annually. Nor must additional licenses be purchased as emergency events unfold. License are sold on a per server basis (unlimited users) and once purchased continue to be valid for the life of the system.

As a browser-based application, WebEOC can be accessed on an intranet and/or over the internet by dispersed participants. Authorized users can access WebEOC from almost anywhere.

The above considerations were the key factors in making a buy decision rather than attempting to build the required functionality.

A Command Post Implementation - Wave

The 45th Space Wing launched the Knowledge Management Initiative (KMI) to provide a common access point for all of the many disparate data sources used to operate the Eastern Range. This resulted in the Knowledge Management Framework (KMF)[3], which was

[2] Anthony J. Simon. *DoD Data Strategy*. Retrieved May 26, 2006 from: http://www.mors.org/meetings/data_practices/data_pres/Simon.pdf

[3] Bimson & Sirmons. Case Study: Deploying and Ontology-Based Enterprise Information Integration at the USAF 45th Space Wing. Retrieved August 18, 2006 from

implemented by Modus Operandi, Inc. using SBIR funds provided by AFRL. The KMF provides applications with the foundation for the Single Integrated Range Picture (SIRP) that is an initiative of the 45th Space Wing. Figure 1 illustrates the KMF's role in providing the foundation for the SIRP[4].

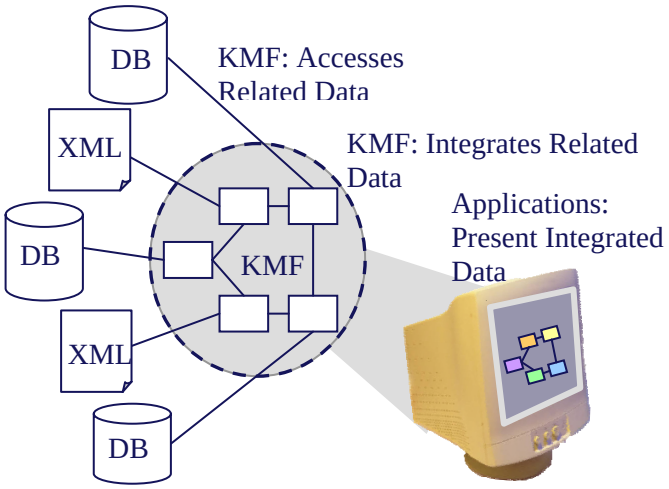


Figure 1. (U) KMF helps realize the SIRP[5]

The KMF has been implemented using MO's Wave product. Wave consists of an ontology layer and associated services implemented on top of BEA's AquaLogic Data Services Platform (ALDSP). Figure 2 illustrates the KMF architecture and indicates the relationship of SCCS to the KMF.

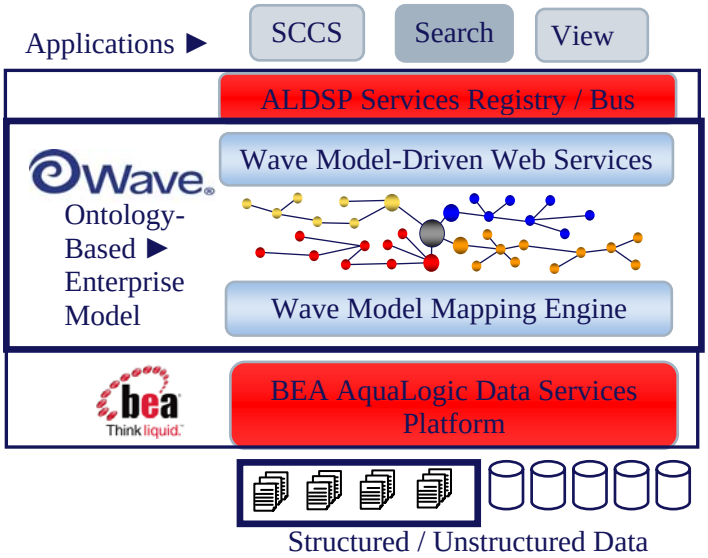


Figure 2. (U) KMF Architecture

The ontology-based enterprise model is created in OWL format using the Protégé modeling tool. The OWL file is then used in BEA WebLogic® Workshop by Wave provided capabilities to create logical data services that can access data sources from which to populate the model with instance data. The logical data services are mapped to physical data sources (which include RDBMS,XML, Java function, and Web Service types of data sources) using ALDSP capabilities. Data transformations can be applied when data is retrieved from a physical data source by a logical data service. Transformations include various math and string functions, as well as custom transformations.[6]

Wave provides a global search capability that can search all mapped data sources to find instance data with terms matching the search terms. Advanced search capabilities are also offered. These advanced capabilities can constrain search results based on membership in a particular class in the ontology model and/or based on the value of an attribute of the class. Wave also supplies a model view capability that allows a user to "walk" relationships among instance data based on the relationships that were created in the ontology model. Using the combination of Wave and ALDSP, applications can access Web services to supply data from multiple disparate data sources and relate the data based on the model. Alternatively, applications can write XQueries and query the KMF directly to obtain data. XQuery allows data to be returned in any XML specified format, so the capability to return data in RDF

http://www.semantic-conference.com/2up_BW/Bimson-Sirmons-bw.pdf#search=%22bimson%20sirmons%22

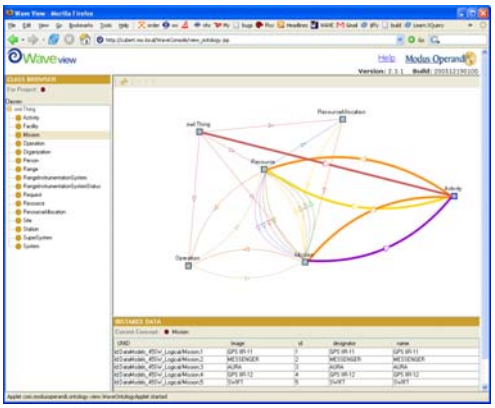
[4] Bimson & Sirmons. op. cit.

[5] Bimson & Sirmons.Ibid.

[6] Robert Price. WebEOC® in Daily Command Post Operations in an Integrated Information Environment at the USAF 45th Space Wing. Retrieved August 25, 2006 from: http://www.modusoperandi.com/downloads/USAF%20and%20WebEOC-Wave%20White%20Paper.pdf

format, for example, is inherent in XQuery. Note that ALDSP does not act as a data warehouse. Data are not pulled from connected data sources and stored on the ALDSP server. Instead, data remains in the source databases and documents and it is accessed when queries are submitted. Frequently accesses data may be cached for performance reasons, but apart from this there is no warehousing of data. Data is returned by ALDSP in the form of XML documents with the structure based on the format derived from the model and the data service. Figure 3 shows Wave Search screens and a screen depicting Wave View, which graphically displays the ontology model with relationships among classes and allows the user to traverse relationships between instances.

Browse integrated data via KMF



Search data via KMF

Figure 3. (U) Wave Search and Wave View[7]

SCCS enhances the situational awareness of commanders in normal day-to-day operations as well as during Battle Staff crisis management situations by obtaining data from the KMF that would otherwise require separate access to multiple data sources. In addition, the ontology framework allows data to be related in ways that may not be apparent from the individual data sources. This means that context can be added to raw data that provides commanders with more meaning. As a result, schedule information, maintenance information, unit status and personnel accountability, geo-spatial data, and airfield operations can all be accessed using SCCS. In addition, Web camera displays and CCTV displays can be shown using capabilities provided in WebEOC.

Adding Mobility

In order to maintain continuity of command post operations in the event of an evacuation from Patrick Air Force Base and Cape Canaveral Air Force Station necessitated by a hurricane or other catastrophe, a mobile capability was deemed critical for the SCCS. When the mobile configuration for SCCS was under development, the requirements were simply, "We want to go anywhere without losing any (or very little) functionality". This presented a considerable challenge. In the information assurance world, this can spell doom for a system and its accreditation since having information leave the .mil boundary is generally frowned upon. As with all systems, all risks cannot be eliminated, but the risks can and should be mitigated to the greatest extent possible. To mitigate the risk to the SCCS and the information it contains, it was decided that the SCCS would not have a connection to any civilian network when mobile and would be under constant control when physically removed from the .mil boundary. In order to provide this support within a reasonable timeline, and for a reasonable amount of money, these requirements were narrowed down to four scenarios:

1. CP moving within the boundaries of PAFB/CCAFS (e.g. to the Alternate CP)
2. CP moving to Malabar annex (with minimal improved facilities and a connection that is not hurricane resistant)
3. CP moving to the Launch Control Center (LCC) at Kennedy Space Center (a Category 4 hurricane rated structure)
4. CP moving to a location physically removed from the CCAFS/PAFB/KSC areas (e.g. Brevard County Emergency Control center or a shelter)

The first two scenarios are considered 'business as usual' as they feature 45 SW LAN connectivity. While Kennedy Space Center's LCC (historically a favorite for hurricane evacuations) is outside of the physical PAFB/CCAFS boundaries, it does feature a connection to the 45 SW LAN. The real challenge to provide the CP with a mobile capability arose in finding a solution to the unknown location in the fourth location requirement. What was developed for the CP was based on having connectivity to the 45th Space Wing LAN or as a stand alone configuration.

[7] Price. Ibid.

During nominal conditions, the mobile server is housed with the CP to provide easy access during a contingency to "grab and go" with the SCCS. To provide system reliability, the primary SCCS/WebEOC server is constantly mirrored to a mobile server. In the interest of providing survivability, the primary server is held at a survivable facility, offering the CP access to the heart of the system from their evacuation point (e.g. the LCC) until infrastructure is effected. Due to the constant mirroring (provided by Double-Take® software) of the database information between the primary and mobile servers, the CP has the latest information upon disconnecting the mobile server from the primary server. In its normal configuration, the SCCS is accessed over the 45 SW LAN (from the primary server). During a network outage or relocation, the mobile server can then be disconnected and operated as a stand alone (what has been dubbed LAN in a Can) system. To enable this switch, the SCCS mobile server is set to DHCP. The LAN in a Can solution provides local area network and WebEOC connectivity. As the technical proficiency of the CP personnel is not always the highest, training aids and clear simple checklists are provided to facilitate the setup of the LAN in a Can. As a stand alone system, the mobile server provides the SCCS environment for the CP (provided by a router and 2 a 20 port switch). The system has been designed for the CP to set up the SCCS environment within minutes with power being the only requirement for operation.

Alternatively, the system can be moved to a facility such as a hotel conference room with Internet connectivity. To keep the mobile server (listed as C in Figure 3) and the information it carries safe, it is kept under constant control and does not connect to the internet. Status reports and other internet needs are generated by the SCCS, composed on one of the CP laptops (D in Figure 3), and sent after physically disconnecting the mobile server (seen as the red dashed line in Figure 3) from the SCCS mobile enclave over a secure VPN connection (provided by a remote base) and exchange account. The laptops are kept secure through firewall software, equipment firewalls (A in Figure 3), and the VPN clients. If an internet connection is not available, using a satellite phone to make the report is an option for the CP.

The SCCS needed to be certified, causing a request to be generated for the WebEOC software to be listed on ITRM, and for the system to be accredited. With security taken into consideration, and the SCCS never truly seeing a non-.mil boundary, accreditation was within reach. The SCCS is classified as a MAC 2 – CL-sensitive system. Figure 3 illustrates the mobile SCCS configuration.

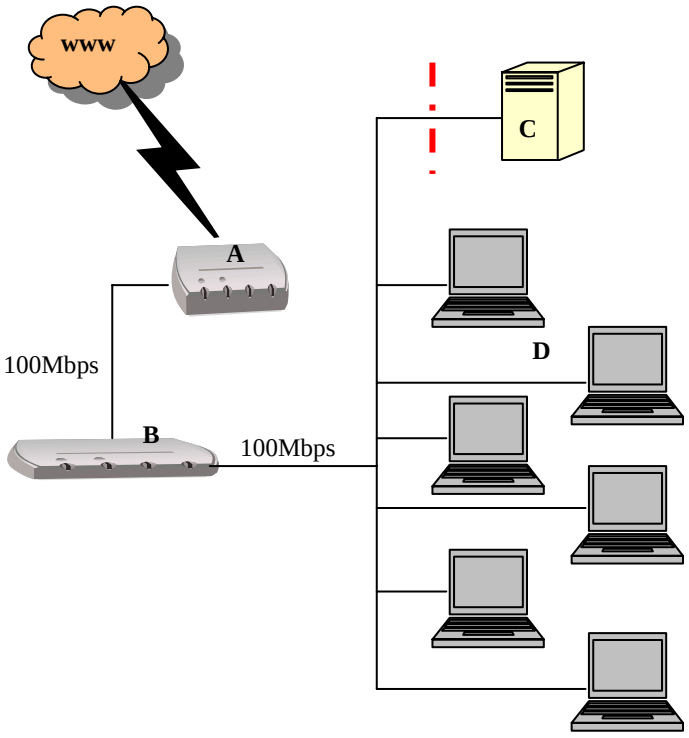


Figure 4. (U) Mobile network with server and laptops

The following scenarios describe the mobile capabilities in more detail.

Scenario #1: Strong Category 3 coming just south of Patrick AFB

1. Call is given for PAFB evacuation.
2. CP Team proceeds to LCC, with CP operators bringing the mobile server.
3. The mobile server is set up using the LCC's connection to the 45 SW LAN.
4. Operation is as normal.
5. Hurricane intensifies, and 45 SW LAN is disabled.
6. Mobile server goes into 'LAN in a Can' (or stand-alone) mode allowing CP staff to use the SCCS.
7. Hurricane passes, SCCS continues to be used in stand alone configuration aiding in the recovery effort.
8. Reports are made by satellite phone (if available) until local utilities/connectivity can be restored.
9. Once conditions allow, SCCS is returned to PAFB and the stationary server is synched to the data on the mobile server using Double-Take.

Scenario #2: Strong Category 5 hurricane passing south of Patrick AFB

1. For safety, evacuation is mandated and CP proceeds to a hotel in Jacksonville to ride out the storm.
2. Mobile server is taken with team and operated in stand-alone configuration with no connection to internet.

3. A broadband connection is available. Reports are generated through the SCCS and submitted through broadband [VPN client] to a remote AFB's exchange email.
4. Reports could also be sent over satellite phone, if available.
5. Data repositories are available to the CP team over a community of practice through the Air Force Portal; additional backup is provided through the VPN connection to the remote AFB.
6. Once conditions allow, SCCS is returned to PAFB and the stationary server is synched to the data on the mobile server using Double-Take.

Connecting to the Net-Centric Environment

Connection to other command posts or emergency management centers that use WebEOC is easily done using native capabilities. Data can be posted from one WebEOC installation to another using an http post. SCCS currently does this to share hurricane readiness data and damage assessment data with the Emergency Operations Center for Kennedy Space Center and Cape Canaveral Air Force Station. Both SCCS and the KSC/CCAFS EOC are within the 45th Space Wing LAN. It is envisioned that in the future the 45th Space Wing will need to access data and services from the Global Information Grid (GIG) as well as provide data and services to other users of the GIG. The KMF should provide a means of doing this that will be transparent to SCCS. BEA is a leader in Service Oriented Architecture (SOA) technology and BEA products serve as the backbone for the DCGS (Distributed Common Ground System) Integrated Backbone (DIB). In the future the KMF will use the capability to locate services and data using standard directory implementations (such as UDDI) and metadata catalogs that are already capabilities provided in the BEA WebLogic stack. As long as connectivity to the GIG is provided SCCS should be capable of operating in the Net-Centric world.

Therefore 45th Space Wing is well positioned to become part of the Net-Centric world. Data is made visible by means of the Wave web services that can be registered in UDDI directories. It will also be possible to locate relevant data by using Wave's federated search capabilities. Data is made accessible through federated search and web services provided by Wave. Data is made understandable because it is presented in the context of an ontology that corresponds to the Community of Interest's view of its world. Trustable data is insured by providing data consumers with the path to the data, thereby revealing the sources of the data. Since BEA's architecture is a Service Oriented Architecture and is built around standards such as XML, SOAP, and UDDI, the architecture is open and easily accommodates new applications and services. Security down to the column level is provided by ALDSP and user authentication and authorization are provided throughout the Weblogic stack.

Future Command Post Capabilities

Future Wave capabilities will increase the semantic capabilities of the KMF. The addition of an inference engine that can operate on the OWL model will enable inferencing over the instance data residing in the data sources. This will allow additional relationships and meaning in the data to be exposed to the end users. Support for connecting to unstructured data (e.g. documents) and extracting query results from the documents is also a desirable feature. BEA will continue to develop their SOA technology and the KMF is expected to make full use of the capabilities. A directory of services and increased use of metadata to aid users and applications in finding the data they require are anticipated future additions.

In future releases, WebEOC will be even more adaptable for 24/7 operations. A future capability, called 24/7, is a new venture to produce a WebEOC-based productivity solution for daily operational use. Current ideas for 24/7 include:

- Easier user customization and more support for simple GIS type functionality.
- Provide the ability to create an incident in WebEOC from an event in 24/7. This means that a Battle Staff incident can be started directly from the normal operating environment.
- Provide statistical displays and advanced end of day reports, as well as weekly, monthly, and yearly reports.
- Provide optimization for a single user desktop environment with Message Center, Daily Log, Task Assignment Menu, and weather common on all desktops.

Additional applications that may be accessed from SCCS are expected to be developed in the future. A Wing-wide personnel accountability application that allows personnel to report their location from both on and off post is a future possibility. A "master schedule" capability is already funded. This will provide commanders with current information on all scheduled activities within the 45th Space Wing area of operations. Events such as hazardous operations, exercises, launch operations, distinguished

visitor visits, and airfield operations will all be gathered from a variety of data sources and presented in a user-friendly interface. Funding has also been allocated for a generic reporting capability that will "pull" data from a variety of sources and format it into required reports. The intent is to significantly automate reports such as Situation Reports and sharply reduce the number of personnel hours expended in compiling them. Given the capabilities provided by SCCS and the KMF, application developers can concentrate on developing user-friendly interfaces and performing data analysis rather than spending time and effort trying to access data.

There may be additional communication abilities added to SCCS. Currently SCCS operates on the 45th Space Wing NIPRNet. In concept (pending a security review and accreditation resubmission), the system as configured could be used to communicate over secure lines (SIPRNet) with a TACLANE/Mux on the command post end, and a TACLANE available on the receiving end (e.g. a satellite reporting station or set access point). In effect, the use of Theatre Deployable Communications (TDC) equipment would allow configuration based on the needs of the war-fighter. Typical TDC setup (scalable) includes the P-MUX., BAM (acting as a PBX; STU-IIIs, faxes, modems, RJ 45 connections/segmented LANs), Crypto Module, and Crypto Interface Module (Figure 4).

TDC can be set up (depending on staffing and needs) within a few hours to a couple of days. TDC would include the satellite uplink that it needs to reference, and would be the gateway for the CP to link back to its home if fiber was not available.

Figure 4 details the basic Integrated Communications Access Package (ICAP) wiring diagram. The darker gray boxes (central, bottom) are representative of the SIPRNet connectivity. The LMST/USC-60 is the sitcom terminal.

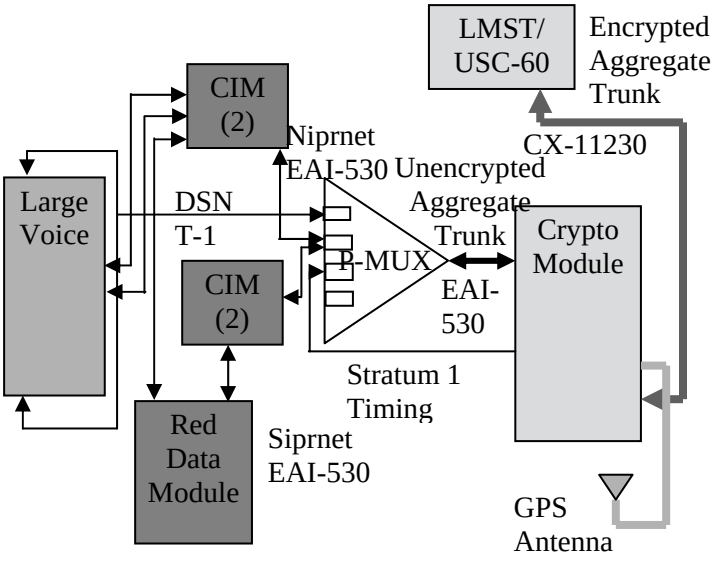


Figure 5. (U) ICAP wiring diagram

Summary

The Shark Command and Control System is a low-cost solution to the 45th Space Wing's command post needs. It offers ease of use, basic capabilities required for most military command posts, and advanced capabilities to access federated data using a domain specific ontology model. SCCS prepares the 45th Space Wing for the Net-Centric environment and, in the future, offers the capability to access data and services from anywhere in the Global Information Grid. The semantic capabilities provided within the Knowledge Management Framework significantly enhance data accessibility and understandability for Wing personnel and offer application developers "one-stop shopping" for their data needs.